NAIC-ID(RS)T-0381-95

NATIONAL AIR INTELLIGENCE CENTER

OVERALL EARLY WARNING ANTIAIRCRAFT JAMMING
TECHNOLOGY IN NATIONAL TERRITORIAL AIR DEFENSE SYSTEMS (II)

**Approved for public release:
distribution unlimited**

Accesion For	
NTIS CRA&I	☒
DTIC TAB	☐
Unannounced	☐
Justification	
By	
Distribution /	
Availability Codes	
Dist	Avail and / or Special
A-1	

HUMAN TRANSLATION

NAIC-ID(RS)T-0381-95 4 December 1995

MICROFICHE NR: 95C000746

OVERALL EARLY WARNING ANTIAIRCRAFT JAMMING TECHNOLOGY IN NATIONAL TERRITORIAL AIR DEFENSE SYSTEMS (II)

English pages: 27

Source: Unknown

Country of origin: China
Translated by: SCITRAN
F33657-84-D-0165
Requester: NAIC/TAEC/Frank Scenna

PREPARED BY:

TRANSLATION SERVICES
NATIONAL AIR INTELLIGENCE CENTER
WPAFB, OHIO

GRAPHICS DISCLAIMER

All figures, graphics, tables, equations, etc. merged into this translation were extracted from the best quality copy available.

OVERALL EARLY WARNING ANTIAIRCRAFT JAMMING TECHNOLOGY IN NATIONAL TERRITORIAL AIR DEFENSE SYSTEMS (II)

5 COUNTERMEASURE METHODS AGAINST EARLY WARNING AIRCRAFT SYSTEMS*

Starting out from the view point of national territorial /25 air defense, the tactical way, with regard to early warning aircraft is to block early warning aircraft detection of targets and to destroy their command and control with regard to operational aircraft.

5.1 Blocking Detection

As far as methods for blocking early warning aircraft detection of targets are concerned--there are hard kill and damage, camouflage, and jamming.

5.1.1 Hard Kill and Damage

Hard kill and damage refers to unmanned aircraft carrying antiradiation missiles attacking early warning aircraft or their escorting aircraft. Due to the long range combat flight areas of early warning aircraft, unmanned craft must possess at least 300-400km of continuous flight capability. In conjunction with this, they should have reconnaissance equipment to guide the flight maneuvers of the unmanned craft in order to avoid the interception of escort aircraft as well as direction finding guidance toward early warning aircraft. Antiradiation missile wave bands are set from ground reconnaissance equipment. The key point is to attack early warning aircraft.

---

* Numbers in margins indicate foreign pagination. Commas in numbers indicate decimals.

5.1.2 Camouflage

The deployment of camouflaged missile positions and tank groups produces large numbers of false targets on early warning radars. It is possible to make on board computers overload.

5.1.3 Jamming

5.2 Blocking Operational Control of Early Warning Aircraft

The objective of jamming is to destroy the early warning radar discovery of our side's interceptor aircraft take offs and flights and to destroy early warning aircraft identification friend or foe with regard to their operational aircraft communications and control and the targets.

5.2.1 Using Active Jamming to Cover Our Side's Interceptor Aircraft Take Offs

When our side's interceptor aircraft take off from outside the range of vision of early warning radars, radars increase the detection range. Normally, they opt for the use of pulse compression technology. They do not employ PD operating modes. At this time, it is possible to opt for the use of frequency shift jamming and noise aimed jamming. When our side's interceptor aircraft enter early warning radar range, radars opt for the use of PD modes of operation. At this time, it is possible to employ narrow band aimed jamming, speed deception jamming, synchronous range and speed jamming, as well as composite types of jamming.

5.3 Jamming Methods Against PD Mode Radars

5.3.1 Jamming Power Calculations

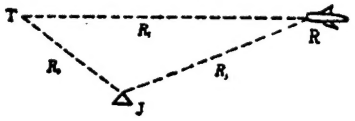
Relative deployment relationships between jammer J, target T, and radar R are as shown in Fig.2. Due to the fact that the

early warning aircraft flight altitude in 9km, it is far smaller than the distance to the forward edge of the battle area. As a result, radars, jammers, and targets are capable of being seen as approximately in the same plane. Radar receiver echo powers are

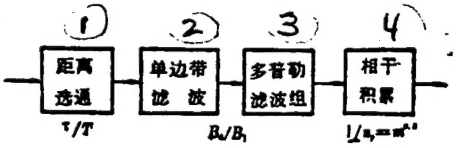
$$P_{r\,i}=\frac{P_t G_t^2 \lambda^2 \sigma}{(4\pi)^3 R_t^4} \tag{1}$$

Radar receiver jamming powers are

$$P_{j\,i}=\frac{P_j G_j G_t' \lambda^2}{(4\pi)^2 R_j^2} \tag{2}$$



(a) Positioning of Jammer (J), Target (T), and Radar (R)



(b) Improvement of PD Radar Signal Handling with Regard to S/J

Fig.2 Jamming of PD Radars

Key: (1) Range Gating (2) Single Side Band Wave Filter
(3) Doppler Wave Filter Components (4) Coherent Accumulation

/26

Receiver input terminal jamming to signal ratio JS is

$$\left(\frac{J}{S}\right)_i=\frac{P_j G_j G_t' 4\pi R_t^4}{P_t G_t^2 \sigma R_j^2} \tag{3}$$

After jamming and signal enter into radar receivers, the jamming to signal ratio will suffer losses. First of all, radars are capable of going through range gating in order to select targets. This generally occurs during target tracking. Next, radars use single side band wave filters gating a carrier frequency spectral line in the vicinity of PRF/2. After that, it is added to the wave filter set. The band width set on wave filters is B_d. Jamming to signal ratio losses are B_j/B_d times (Here, B_j is the jamming band width). We now take the E-3A as an example to calculate jamming loss factors.

The E-3A uses a $\theta_a=0.73^\circ$ azimuth beam width to make 360° mechanical sweeps. Antenna rotation speed is n_a=6r/min. Then, the period of beam loiter on the target direction is $nT_r=\theta_a/6n_a$ =0.01s. Echo signal spectral line width is $B_d = 4/nT_r = 400Hz$.

After signal wave filtering, coherent and noncoherent accumulation is carried out, also giving rise to jamming to signal ratio losses. Accumulation processes are divided into two steps. The total number of pulses within the stop over time is divided into m sets. Within each set, pulses are handled coherently. Between sets, pulses make noncoherent accumulations. When radars are at medium and high repetition frequencies, the pulse numbers associated with coherent accumulations are respectively 2^4-2^6 and 2^9-2^{11} .

E-3A's opt for the use of high repetition frequencies (30-200kHz). Assuming that PRF = 100kHz, then, the number of pulses within loiter times is $N=0.01\times100\times10^3=1000$. If $n_p=2^9$, then, N pulses are divided into m=2 sets. PD handling gives rise to jamming to signal ratios with total losses which are

$$L=\frac{B_j}{B_d}n_p m^{0.8}=2\times10^6 \qquad (4)$$

Actual losses are 10^5 (50dB). In this way, it is possible to obtain a final expression for accumulator output jamming to signal ratios

$$(J/S)_o = (J/S)_i \frac{1}{L} \gamma_1 \tag{5}$$

Effective jamming conditions are

$$(J/S)_o \geq K_1 \tag{6}$$

In this inequality K_1 is a coefficient larger than 1. It stands for the jamming to signal ratio required for effective jamming and is called the suppression coefficient. γ_1 is the jammer polarization coefficient. E-3A radar parameters are substituted into the equations above, and it is possible to calculate that the effective radiated power associated with jamming a single early warning radar to be 10^7 - 10^8 W.

5.3.2 Narrow Band Noise Aimed Jamming

The jamming band widths which should be employed are only narrow band aimed type jamming associated with a few multiples of Doppler wave filter band widths. This type of jamming requires that frequency detection and guidance accuracies are both high. Realization is only possible opting for the use of medium frequency locked phase technology.

5.3.3 Speed Deception Jamming

The main jamming method associated with PD is radar speed deception, that is, first using amplifier link transceiver signals to cause radar speed gate tracking jamming. After that, use is made of a fixed pattern to increase the Doppler frequency shift and cause speed gate tracking jamming movements. After that, reception is stopped. During speed deception, the

selections of skip frequencies, tractive speeds, as well as nontractive, tractive, and shutoff periods are key.

5.3.4 Doppler Frequency Block or Doppler Random Wobble Jamming

The results of this type of jamming will make speed gate tracking unstable.

5.3.5 Range and Speed Synchronous Jamming

Tractive range jamming of PD radars must be synchronous with speed deception jamming. First of all, typical delay line storage frequency tractive range jamming is not effective against PD radars. The reason is that the frequencies which this type of jamming transmits signals at have comparatively large errors existing between them and radar frequencies. They are equivalent to the relatively large sudden Doppler changes which exist, causing speed gates not to be influenced by jamming. As a result, range gates also have no influence on jamming. Next, PD radars are capable of using comparisons between false target range characteristics and true target speed characteristics (or false target speed characteristics and true target range characteristics) in order to discover false target tractive distance deception. With regard to PD radars which possess highly dynamic states and do not opt for the use of AGC, when realizing tractive range jamming, there is generally no need for traction stop periods, that is, there is immediate jamming traction after capturing echoes. Synchronous traction must satisfy

$$S = v_0 + \frac{1}{2}at^2, \qquad v = v_0 + at \tag{2}$$

5.3.6 Composite Jamming

Composite jamming is nothing else than making use of active, wide band jamming signals to irradiate foil strip clouds. In conjunction with this, there is scattering in the direction of the radar. At this time, the foil strip noise spectrum received by radars widens out and is stronger than moving target echoes, causing radars to have no way to pick out moving target information from the foil strip background.

5.4 Jamming Methods Against Pulse Compression Radars

5.4.1 Jamming Power Calculations /27

Considering the geometrical relationships between jammers, targets, and early warning radars as shown in Fig.3, at this

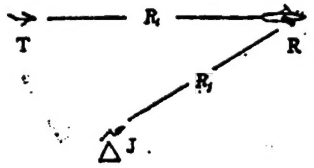


Fig.3 Placement of Jammer, Early Warning Aircraft, and Target

time, radar receiver input terminal jamming to signal ratio is $(J/S)_1$. With regard to signal compression handling, radars cause D fold jamming to signal losses. D is the radar pulse compression handling gain. At this time, the receiver output jamming to signal ratio is

$$(J/S)_0 = (J/S)_1 \frac{B_1}{B_r} D\gamma_1 \qquad (7)$$

Taking E-3A AN/APY-2 parameters and substituting into equation (6), it is possible to solve for the jamming cover zone range. When calculating, compression ratios associated with

linear frequency adjustment signals use E-2C radar data, that is, D=59. During long range detection, radars do not use PD operation modes. Therefore, option is made for the use of noise aimed jamming. When calculations are made, jamming band width is 18MHz. Radar receiver band width is 6MHz.

5.4.2 Cover Pulse Jamming

Cover jamming is also called range gate jamming. Jammers begin producing pulses before echoes arrive. In conjunction with this, these wide pulse cover echoes run for a certain period of time after they exceed echo pulses. Pulses are capable of using carrier frequency constant wide pulses and are also capable of using a band of noise modulated frequency.

Cover jamming is used to lower radar range resolution. When jamming is a constant frequency, pulses are not compressed. Compression wave filter output is still pulses of equal amplitude. Moreover, after LFM signal compression, one has the appearance of a main compression lobe and two time interval side lobes. Due to the linear and additive nature of compression wave filters, jamming pulses and LFM signal outputs will add with each other as vectors. Because of the existence of time interval side lobes and the phase differences of jamming pulses between compression pulses, the top parts of cover pulses are not smooth but go up and down. Undulation amplitudes are generally not great. When J/S is adequately large, cover pulses will overspread echo signals. Using cover pulses associated with noise modulated frequencies for jamming has better results than ordinary cover pulse jamming. The cover pulse realization diagram is as shown in Fig.4.

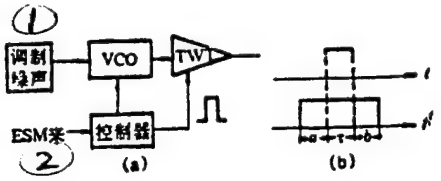


Fig.4 Noise Cover Pulse Jamming

Key: (1) Modulation Noise (2) Coming ESM (a) Control Device

5.4.3 False Target Jamming

False target jamming is noise + pulse jamming. When noise jamming submerges echo signals, use is made of a different jamming gate to produce false pulses at different ranges. Due to signal pulse widths being very narrow constant frequency pulses after compression (generally, 0.2-0.4 microseconds), as a result, false target pulses are not necessarily LFM or phase code signals but are ordinary pulses with pulse widths larger than or equal to compression pulse widths.

The method for realizing this type of false target jamming is as shown in Fig.5.

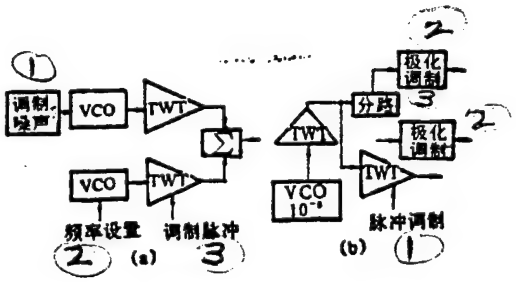


Fig.5 False Target Jamming

Key: (a) (1) Modulation Noise (2) Frequency Setting (3) Modulation Pulse; (b) (1) Pulse Modulation (2) Polarized Modulation (3) Shunt

5.4.4 Shifted Frequency Jamming

Shifted frequency jamming is a type of transmission jamming. After jammers receive radar irradiation pulses, frequency modulation is gone through, and they are transmitted back to the radar. Shifted frequency jamming has different jamming effects on different pulse compression radars.

a. Jamming with Regard to LFM Radars

A strong coupling exists in linear modulated frequencies in time and speed. When echo signals possess Doppler frequency shift f_d, compression signals will displace Δt. There are the relationships set out below between Δt and f_d. /28

$$\Delta t = -\frac{2\pi f_d}{\mu} = \frac{T f_d}{B} \quad (8)$$

In the equation, B is the frequency shift within pulses. T is linear modulated frequency pulse width. As a result, when frequency shifted jamming acts on compression filters, jamming compression pulses will appear before echo pulses or after them. This is determined by shifted frequency polarity. Changing the magnitude of f_d, it is possible to produce range traction. Changing the magnitude and polarity of f_d, it is possible to make range gate tracking unstable. Traction ranges are smaller than the width of wide radar transmitted pulses. As far as the jamming effects of shifted frequency jamming on linear modulated frequency radars are concerned--besides range traction--there are also false target and range gate random wobble effects.

b. Jamming Effects on Phase Code Signals

Phase codes often used are two phase codes (Bake ((phonetic)) code and M array code). When shifted frequency jamming impacts Bake (phonetic) code, one will have the

appearance of paired compression peaks. Following along with increases in shifted frequencies, jamming energies will gradually move from one set of peaks to another set of peaks. The time interval between peaks is the minor pulse width. However, when shifted frequencies are adequately large, jamming peaks will become lower, and echoes will increase in strength. As a result, when realizing shifted frequency jamming against corresponding code signals, it is necessary to increase supplementary modulation in order to inhibit one jamming peak and increase another jamming peak.

When implementing shifted frequency jamming against M array code, frequency shifted jamming will produce a set of random jamming peaks. The interval between jamming peaks will be determined in the same way by pulse width. However, following along with increases in frequency shifts, jamming peak distribution ranges expand, forming cover type jamming. With regard to Frank four phase code shifted frequency jamming, a set of wide jamming lobes will appear. When J/S is large, these jamming lobes not only cover target echoes. Moreover, false targets appear. Realizing shifted frequency jamming technology methods and speed deception is the same. At this time, f_d = 1-2 MHz.

5.5 Distribution Type Jamming

If one wants to jam modern early warning radars, it is necessary to produce megawatt level jamming powers. To this end, it is possible to opt for the use of the several types of technology set out below: high power phase control array jamming technology, high power multiple beam jamming technology, multiple single tube synthetic power synthesis technology, and jamming technology associated with power produced by single high power tubes. The drawbacks associated with these jamming technologies are not being advantageous to producing multiple false targets

against early warning radar main lobes, not being advantageous to the forming of large jamming fans, and the ease of making use of passive positioning to obtain jammer locations and suffer antiradar missile attacks. In this connection, it is possible to opt for the use of distributed type jamming technology. That is, in the direction of AEW early warning radar observation, use a certain pattern of distribution to arrange multiple sets of jammers.

6.5.1 Uniform Linear Array Distribution Form

Assume that N+1 jamming sources are arranged in a linear array in accordance with the distance L, as shown in Fig.6.

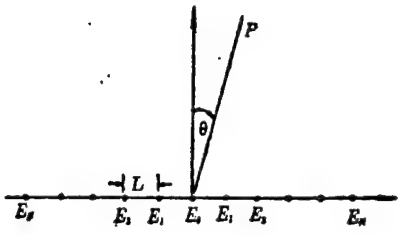


Fig.6 Uniform Linear Array Distribution

$$E_\theta = E e^{j\omega t}$$

The nth source at point P in space, relative to E_0, has phase shift

$$\varphi_{n+} = (2\pi/\lambda) n L (1 - \sin\theta)$$
$$\varphi_{n-} = (2\pi/\lambda) n L (1 + \sin\theta)$$

Assuming that the various jamming amplitudes at point P in space are all the same, then, it is possible to solve for the resultant field associated with point P

$$|J| = E\left\{1 + \sum_{n=1}^{N} \exp\left[j(2\pi/\lambda) nL \cdot (1-\sin\theta) \right] + \sum_{n=1}^{N} \exp\left[j(2\pi/\lambda) nL(1+\sin\theta) \right]\right\} \quad (9)$$

5.5.2 Two Uniform Linear Array Vertically Constituted Planar Arrays

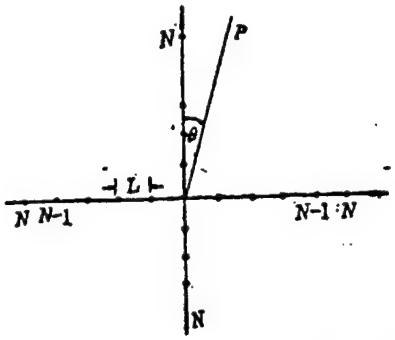


Fig.7 Two Uniform Linear Array Vertically Constituted Planar Arrays

/29

Planar jamming arrays are composed of 4N+1 individual jamming sources (Fig.7). The resultant field at point P in space

$$|J| = E\left\{1 + \Sigma\exp\left[j(2\pi/\lambda) nL \cdot (1-\sin\theta) \right] + \Sigma\exp\left[j(2\pi/\lambda) nL\,(1+\sin\theta) \right] + \Sigma\exp\left[j(2\pi/\lambda) nL\,(1-\cos\theta) \right] + \Sigma\exp\left[j(2\pi/\lambda) nL(1+\cos\theta) \right]\right\} \quad (10)$$

5.5.3 Jamming Effects

a. In accordance with a certain pattern of arrangement, it is possible to synthesize in space high powers. This guarantees to supply power for jamming early warning radar ancillary lobes as well as multiple base radars.

b. Due to resultant field distortions produced in front of phase waves, when early warning aircraft, therefore, opt for the use of single pulse tracking, the jamming results are also clear.

c. Jamming means are flexible and varied. They can make war separately. They can also cooperate in jamming. As a result, it is possible to jam multiple targets.

5.6 Jamming Platforms

Jamming of early warning radars can make use of various types of jammer platforms--for instance, ground jammers, shipborne jammers, airborne jammers, and satellite borne jammers.

6 JAMMING OF AEW COMMUNICATIONS SYSTEMS

6.1 Jamming of Communications Electronics Equipment Related to AEW

The carrying out of jamming against communications electronics equipment related to AEW is another important way of jamming AEW. Among these--in particular, jamming communications and identification friend or foe systems--is the key to destroying AEWC 31. Modern communications opts more and more for the use of expanded frequency technologies. Among these, skip frequency and direct array expanded frequency communications are commonly used modes of operation--in particular, the utilization of skip frequency communications is more extensive. Skip frequency communications frequencies change in accordance with false random codes. In this way, intercepting skip frequency communications is even more difficult than intercepting conventional frequency communications. Due to skip frequency communications opting for the use of digital technology, they possess a high degree of security. Even through intercepts of station signals, there is still no way to obtain useful intelligence. It is only significant if analysis and

identification is done on multiple communications networks (station stepped) existing at the same time, as well as azimuths measured, threat levels determined, and effective jamming is carried out. This requires nothing else than that skip frequency countermeasures equipment possess capabilities for fast acquisition, analysis, and identification of signals.

6.2 Block Type Jamming Against Expanded Frequency Communications

6.2.1 High Speed Communications

Information is stored ahead of time. When transmitted, it is sent out within extremely short periods of time using high transmission rates. They use widened signal frequency spectra in the frequency realm in order to shrink communication durations in the time realm. The peculiarity of barrage type jamming is the ability to carry out effective jamming in a very wide frequency domain. As a result, with regard to all the high speed communications appearing within this very wide frequency domain, so long as they are within the jamming time period--no matter how fast communications speeds are--it is then possible to carry out effective jamming in any case.

6.2.2 Skip Frequency Communications

During communications, the various sides of the communication all automatically switch the communications frequencies synchronously within a certain frequency band. Moreover, frequency domains during the entire communications process are very greatly expanded compared to fixed frequency communications. Barrage jamming is capable of effectively jamming all fixed frequency communications within its very wide jamming frequency band. In the same way, it is capable of carrying out effective jamming against all skip frequency communications within its very wide jamming frequency band. As far as the skip frequency gain presented by skip frequency

communications within frequency domain extensions is concerned--under barrage jamming conditions--it has already been offset by barrage jamming power multiplier values. So long as jamming frequency widths are larger than skip frequency widths, that is, barrage type jamming multiple values are larger than skip frequency multiplier values--no matter how high skip frequency speeds are, how long skip frequency arrays are, how concealed synchronous signal transmissions are--barrage type jamming is capable, in the same way, of carrying out effective jamming against it.

6.2.3 Direct Array Expanded Frequency Communications

Narrow frequency band bs information--at communications transmission terminals--makes use of high speed false random code modulation to change it into broad frequency band Bs information to transmit out. At reception terminals, after wide frequency band signal frequencies and basic amplitudes modulated by the use of synchronous false random codes are mixed together, narrow band information is also returned and received. From this is produced the extended frequency gain $G=B_s/b_s$. In the same way, in situations with barrage type jamming, this extended frequency gain is offset by the barrage type jamming power multiplier value n. When communications terminals are fixed frequency communications and power jamming/signal ratios are 1, jamming is effective. When fixed frequency communications are changed to extended frequency communications, if the frequency band expansion is 100 fold, that is, the extended frequency gain is 20dB, then, so long as jamming and signal power ratios increase 100 fold, then--and only then--is jamming effective. This recapture from wide band extended frequency signals through receivers is narrow band signals, caused by signal powers passing through narrow band filters uninhibited. In order to guarantee effective jamming, jamming band widths must expand 100 fold.

Only then is it possible to guarantee the jamming/signal power ratios within each basic band width being 1.

/30

As a result, barrage jamming is capable of effective jamming of all fixed frequency communications within the very wide jamming frequency bands. In the same way, it is possible to carry out effective jamming against all direct array expanded frequency communications within the very wide jamming frequency bands. No matter how high the modulation speeds are or how long the modulation arrays are, so long as the signal frequency widths after their modulation are within barrage type jamming frequency widths, then it will work.

It is possible to see from the above that, provided we know the signal jamming ratio ß that enemy communications receivers are set on, and, in conjunction with that, option is made for the use of corresponding jamming frequency band coefficients γ (the ratio between jamming band width B_j and expanded frequency band width B_s), it is then possible to create reception signals producing code error rates of 10^{-2} or better. Therefore, code error rates are functions of ß and γ, recorded as

$$P_0 = f(r, \beta) \tag{11}$$

When ß = 0dB, that is, when the jamming signals and the extended frequency signals receivers are placed on possess the same electrical levels--for $\gamma > 0.5$--it is possible to produce error code rates of 10^{-2} or better. If effective powers P_j of jammers are smaller than the product of the skip frequency channel number M and signal powers, then, jammer powers concentrated on a certain portion of the overall skip frequency band will be relatively effective. This is nothing else than what is called partial frequency band jamming.

Let P_i stand for the overall jamming power used against M channels. Following along with increases in jamming channel numbers M_i--speaking in terms of each channel receiving jamming--available jamming powers will then fall. If jamming powers are uniformly distributed, and these signals are not duplicative of each other, then, the jamming power on each channel is $P_{j_i}=P_j/M_j$. The number of channels receiving jamming is

$$M_j = \text{int}(\mu M) = \text{int}(\mu M \cdot \omega / C) \tag{12}$$

In equations, (C, γ) is a code group, that is, taking a ω bit code to carry out coding, one obtains each C code bit to send out. M_μ stands for the number of channels that have not been coded and are available for use. $\mu = M_i/M \leq 1$.

When the jamming power in channels receiving jamming approximates signal powers, one will have the appearance of maximum bit errors. As a result, it is possible to anticipate optimal μ values to be

$$\mu_0 = \begin{cases} \dfrac{P_j}{P_s M}, & P_j < P_s M \\ 1, & P_j \geq R_s M \end{cases} \tag{13}$$

6.3 Repeating Type Jamming Against Communications Systems

Traditional repeating type jamming is a single frequency aimed type jamming, that is, reconnaissance and processing are gone through with regard to communications signals. After that, a jamming signal is transmitted with the same frequency as the signal. As far as the carrying out of effective jamming against skip frequency communications is concerned, it is necessary to make jamming signals reach receivers in the skip frequency signal halt period. Moreover, jamming signals should possess optimal jamming forms. This is nothing else than requiring that jammers understand the transient frequency characteristics associated

with skip frequency signals and that jammers be capable of rapid tracking of skip changes in frequency.

The geometrical arrangement associated with skip frequency communications transmitters and receivers and repeating type jammers is as shown in Fig.8. In order to make jammers effective, it is necessary to satisfy

$$\frac{d_2+d_3}{c}+T_p\leqslant\frac{d_1}{c}+\eta T_d \tag{14}$$

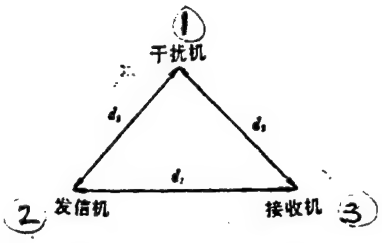


Fig.8 Skip Frequency Communications Transceiver and Jammer Placement

Key: (1) Jammer (2) Transmitter (3) Receiver

In the inequality, c is the speed of electric wave propagation. T_p is reconnaissance and processing time. T_d is signal halt time. η is a constant smaller than 1.

When repeating type jammers are placed within an ellipse with transmitter and receiver as foci, if $T_p < \eta T_d$, then, relationship (14) always applies.

Due to the fact that repeating jamming requires processing time as well as geographical location, there exists a jamming signal time delay associated with these signals and skip frequency signals received by communications receivers. This time delay is

$$T_{sj} = \min(T_p + \frac{d_2 + d_3 - d_1}{c},\ T_d) \qquad (15)$$

Effective jamming time is then $T_{sj} = T_d - T_{sj}$. As a result, only when $T_{sj} < T_d$ will jamming be effective.

/31

Assume that skip frequency signal reconnaissance intercept probability is P_1 and jammer probability of jamming intercepted skip frequency signals is P_2. Then, the probability of skip frequency signals receiving jamming is $P_j = P_1 P_2$. The probability when jamming is not received is (1-P). Again, assume that the code error rate for skip frequency communications under jamming conditions is F_j and the code error rate when there is no jamming is F_{nj}. Obviously, there is a relationship between code error rate F_j and jamming signal ratios for receivers. Moreover, F_{nj} and signal to noise ratios at receivers are related. Therefore, the code error rate in periods when jamming exists is $[P_j F_j + (1-P_j)F_{nj}]$. In periods when there is no jamming, the code error rate is F_{nj}. Therefore, average code error rates are

$$P_a = \frac{T_d - T_{sj}}{T_d} P_j F_j + (1 - \frac{T_d - T_{sj}}{T_d} P_j) F_{sj} \qquad (16)$$

Due to $F_j > P_a > F_{nj}$, P_a is, therefore, a reduction function of T_{nj}. In order to reach effective jamming, from equation (15), it is possible to know that

$$T_{sj} = T_p + \frac{d_2 + d_3 - d_1}{c} \qquad (17)$$

From equation (16), one gets

$$T_p = T_d - \frac{T_d(P_0 - F_{sj})}{P_j(F_j - F_{sj})} \qquad (18)$$

In order to make jamming produced code error rate P_a exceed a certain anticipated value Pao, that is $P_a > P_{a0}$ --from equation (17) and (18)--it is possible to obtain upper limit values for reconnaissance and processing signal times

$$T_{j\cdot} \leqslant T_{\cdot} - \frac{T_d(P_{\cdot o} - F_{\cdot i})}{P_j(F_j - F_{\cdot i})} - \frac{d_2 + d_3 - d_1}{c} \tag{19}$$

As far as repeating jamming is concerned, under conditions of skip frequency speed increase and skip frequency multiple address signals (each skip frequency net), jamming effects will decrease. Methods for overcoming this are to opt for the use of multiple repeating type jammers respectively carrying out specially designated signal jamming and to opt for the use of wide band repeating type jammers. Based on communication signal characteristics, appropriate modulation is added.

6.4 Cover Type Jamming Against Voice Communications

Voice communications are one of the key forms of communications employed at the present time in AEW communications systems. With regard to jamming results associated with voice communications, they are manifested as drops in the degree of clarity associated with receiver output terminal voice. Readability is determined by ear. It is the result of the physiological/psychological sense of human hearing. Covering jamming is the primary method of jamming against voice communications. After being subjected to covering jamming, the degree of voice readability will clearly drop. There are two kinds of covering type jamming--noise modulation jamming and acoustic noise jamming.

6.5 Pulse Jamming Against Communication Systems

With regard to the jamming of digital communications, pulse jamming is the most effective form of jamming. It is capable of making code error rates clearly increase.

Bit errors given rise to by pulse jamming show up in large numbers. If jamming pulse widths and the width of a piece of code are the same, then, even if option is made for the use of

error correction code, it is still not possible to clearly lower character error probabilities.

6.6 Frequency Shift Jamming Against Communication Systems

Frequency shift telegraphy has very strong counter jamming capabilities in communications. Frequency shift jamming signals have good jamming effects against frequency shift keying (FSK) controlled signals and are optimum jamming forms. At the same time, frequency shift jamming also has good jamming effects against continuous wave telegraphy and amplitude modulation telegraphy.

In frequency shift jamming, the size of frequency shifts is directly related to jamming results. If frequency shift deviations are too small, then, the transmission frequency range is narrow. Experienced operators are capable of using tuning methods to easily avoid jamming signals. If frequency shift deviations are excessively large, then, jamming signal energies are dispersed, severely influencing jamming results. As a result, when opting for the use of frequency shift jamming, frequency shift deviations have an optimum range.

Under conditions where frequency modulation index m > 1, frequency band B_i is approximately

$$B_i = \Delta f + 2F$$

In the equation, Δf --- maximum frequency shift deviation
F --- modulation frequency.

The relationship between frequency band width B_j and the number of side frequencies n is $B_j = 2F \cdot n$. Moreover, n should be selected as

$$n = \sqrt{m^2 + \frac{2}{\pi} am} \tag{20}$$

Here, a is a constant selected with a relationship to side frequency amplitude

$$\frac{1}{a} = \frac{1}{(m^2 - n^2)\pi}$$

/32

When designing frequency shift jamming, Δf=3-5kHz is optimum.

7 JAMMING OF IDENTIFICATION SYSTEMS

The third way of jamming is to carry out jamming of identification friend or foe systems. The effect of the jamming is to make early warning aircraft systems have no way of identifying friend or foe, blocking the control of operational aircraft.

At the present time, early warning aircraft identification friend or foe systems are mainly MKX II's. These are pulse position modulated and used in conjunction with pulse time delay coincidence type operating, that is, transmitting instantaneous signals of three pulse coding. After response devices on combat aircraft receive query signals, they carry out pulse width discrimination and pulse delay duplication, triggering response devices in order to produce 16 bit displacement key control code. When querying devices on early warning aircraft receive reply signals, they also do time delay duplication, producing the queried target's bright arc on radar display devices.

With regard to jamming of pulse position modulated signals, it is comparatively easy. Jamming to disrupt pulses has relatively good results. When noise band widths associated with producing disrupted pulses are selected appropriately, they have very high coincidence probabilities, making query device outputs

produce a series of bright arcs on radar display devices. Thus, there is no way to distinguish friend or foe.

8 COUNTERMEASURE SYSTEMS TO COUNTER EARLY WARNING AIRCRAFT

The systems in question are composed of a line and block chart as shown in Fig.9. They are composed of sensor elements,

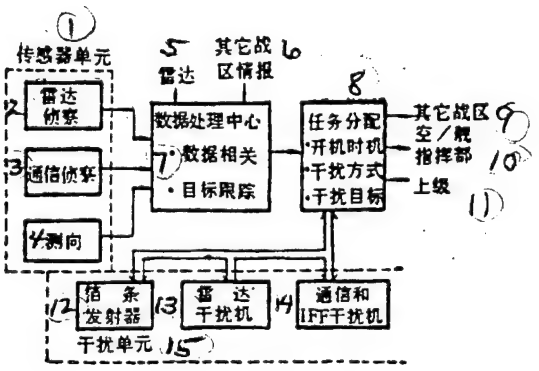


Fig.9 Composition of Countermeasure Systems

Key: (1) Sensor Units (2) Radar Reconnaissance (3) Communications Reconnaissance (4) Direction Finding (5) Radar (6) Other Theater Intelligence (7) Data Processing Center - Data Correlation - Target Tracking (8) Task Distribution - Start Time - Jamming Mode - Jamming Target (9) Other Theater Air/Naval (10) Command Section (11) Higher (12) Foil Strip Launchers (13) Radar Jammers (14) Communications and IFF Jammers intelligence (data) processing elements, task distribution elements, and jamming elements.

a. Sensor Elements

They are used in detecting and identifying early warning aircraft and combat aircraft, analyzing communications and identification friend or foe signals. Sensor elements are composed of radar reconnaissance equipment, communications reconnaissance equipment, and direction finding equipment.

Radar Reconnaissance This primarily detects the existence and intentions of early warning aircraft. When early warning aircraft go into an operational configuration, they normally circle within a fixed range of distances (for example, 150-170km from the forward edge). In conjunction with this, they detect fixed and moving military targets within the combat zone. On the basis of radar wave bands and parameters, comparisons are made with parameters existing data bases, and early warning aircraft are identified. Due to the fact that early warning aircraft are capable of operating beyond visual range (reconnaissance equipment should, as much as possible, be placed along the forward edge of the combat zone, increasing the detection range). There is no way to precisely determine whether or not have gone into an operational configuration. To this end, it is necessary that radars supply the distance of early warning aircraft from the combat zone. In conjunction with this, identifications of them must be carried out. Besides this, radar reconnaissance equipment is also used to discover bombers and attack aircraft guided by early warning aircraft, carrying out reconnaissance and analysis on early warning aircraft identification friend or foe signals.

Communications Reconnaissance Equipment Used to measure communications frequencies and modes as well as to guide communications jammers.

Direction Finding Equipment Direction finding, positioning, and tracking of early warning aircraft by multiple direction finding receivers. In conjunction with this, combat intentions of early warning aircraft are analyzed from them. Besides the sensor data discussed, information coming into systems is also capable of coming from radars and other theater intelligence.

b. Data Processing Elements With regard to correlations associated with data coming from various sensors as well as the matching of parameters associated with early warning aircraft in data banks and the identification of early warning aircraft, aircraft attacking early warning aircraft are tracked in order to aim jammers in direction and frequency. The processing elements in question are composed of computers and data bases.

c. Task Distribution Elements They are used to control the operations of one type or several types of jamming systems. They regulate start times and jammer directions and parameters, realizing azimuth and frequency guidance.

In one theater direction, there are normally several early warning aircraft participating in precombat control. In particular, when the direction of attack is from the sea toward the land, it is possible to have antisubmarine P-3 early warning aircraft as well as E-2C/E-3A's operating together to monitor the land and sea. It is also possible to have the same type of early warning aircraft participate in controlling combat from different directions. As a result, task distribution is the key to being able to counter early warning aircraft or not.

Task distribution elements must also determine jamming element start times on the basis of the distance of early warning aircraft from the forward edge of the battle area. Early warning aircraft flight altitudes are approximately 9000m. Their line of sight is 389km. Jamming elements are only activated provided they have entered into line of sight range.

Task distribution elements store within themselves various types of jamming system power range parameters in order to correctly select for use jamming methods and jammer combinations

(for example, multiple jammers jamming the same early warning aircraft).

Besides this, task distribution elements should also have feedback from jamming elements of such information as assets occupied and remaining.

d. Jamming Elements Used to construct foil strip protective screens. Jam early warning radars, command communications, identification friend of foe, as well as various types of navigation systems.

The utilization of jamming elements should be realized in stages. Before early warning aircraft enter into command of combat operations, use foil strip launchers to construct a foil strip screen area in the vicinity of the forward edge. Before enemy attack planes enter into the forward edge of the battle area, use radar jammers to jam early warning aircraft monitoring radars. After attack planes have entered into the forward edge of the defensive area, use communications /IFF jammers to destroy the command communications.

REFERENCES

1 Long M W. Airborne cariy warning system concept. Artech House Boston, 1991

2 Boyle D. Airborne early warning two, major system for Europe. Interavia, Aug. 1980

8 A leacy, AEW, nimrod, the mission system arionics. IEEE proc, Vol. 128, No. 7, Dec. 1981

DISTRIBUTION LIST

DISTRIBUTION DIRECT TO RECIPIENT

ORGANIZATION	MICROFICHE
B085 DIA/RTS-2FI	1
C509 BALL0C509 BALLISTIC RES LAB	1
C510 R&T LABS/AVEADCOM	1
C513 ARRADCOM	1
C535 AVRADCOM/TSARCOM	1
C539 TRASANA	1
Q592 FSTC	4
Q619 MSIC REDSTONE	1
Q008 NTIC	1
Q043 AFMIC-IS	1
E404 AEDC/DOF	1
E410 AFDTC/IN	1
E429 SD/IND	1
P005 DOE/ISA/DDI	1
1051 AFIT/LDE	1
PO90 NSA/CDB	1

Microfiche Nbr: FTD95C000746
NAIC-ID(RS)T-0381-95